日本国特許庁 JAPAN PATENT OFFICE

01.12.2004

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

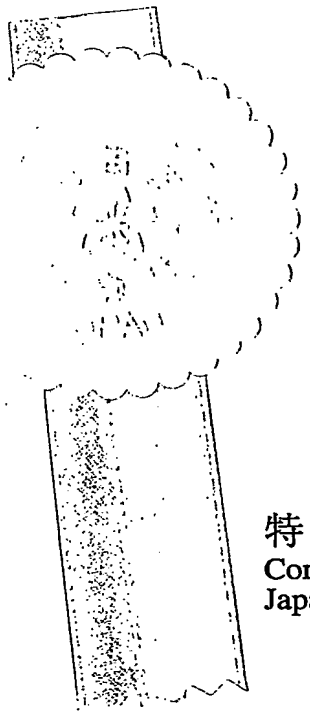
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年１２月　１日

出願番号
Application Number: 特願２００３－４０１３８３

[ST. 10/C]: [ＪＰ２００３－４０１３８３]

出願人
Applicant(s): 松下電器産業株式会社



２００５年　１月１３日

特許庁長官
Commissioner,
Japan Patent Office

小川洋

出証番号　出証特２００４－３１２２１７４

【書類名】　特許願
【整理番号】　2048150065
【特記事項】　特許法第３６条の２第１項の規定による特許出願
【提出日】　平成15年12月 1日
【あて先】　特許庁長官殿
【国際特許分類】　G06F 17/00
【発明者】
　【住所又は居所】　シンガポール５３４４１５シンガポール、タイ・セン・アベニュー、ブロック１０２２、０６－３５３０番、タイ・セン・インダストリアル・エステイト、パナソニック・シンガポール研究所株式会社内
　【氏名】　ジ・ミン
【発明者】
　【住所又は居所】　シンガポール５３４４１５シンガポール、タイ・セン・アベニュー、ブロック１０２２、０６－３５３０番、タイ・セン・インダストリアル・エステイト、パナソニック・シンガポール研究所株式会社内
　【氏名】　ファング・ゾンヤン
【発明者】
　【住所又は居所】　シンガポール５３４４１５シンガポール、タイ・セン・アベニュー、ブロック１０２２、０６－３５３０番、タイ・セン・インダストリアル・エステイト、パナソニック・シンガポール研究所株式会社内
　【氏名】　シェン　メイ・シェン
【発明者】
　【住所又は居所】　シンガポール５３４４１５シンガポール、タイ・セン・アベニュー、ブロック１０２２、０６－３５３０番、タイ・セン・インダストリアル・エステイト、パナソニック・シンガポール研究所株式会社内
　【氏名】　リュウ・ジン
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　妹尾　孝憲
【特許出願人】
　【識別番号】　000005821
　【住所又は居所】　大阪府門真市大字門真１００６番地
　【氏名又は名称】　松下電器産業株式会社
【代理人】
　【識別番号】　100086405
　【弁理士】
　【氏名又は名称】　河宮　治
　【電話番号】　06-6949-1261
　【ファクシミリ番号】　06-6949-0361
【選任した代理人】
　【識別番号】　100098280
　【弁理士】
　【氏名又は名称】　石野　正弘
　【電話番号】　06-6949-1261
　【ファクシミリ番号】　06-6949-0361

【手数料の表示】
　【予納台帳番号】　163028
　【納付金額】　35,000円
【提出物件の目録】
　【物件名】　外国語特許請求の範囲　1
　【物件名】　外国語明細書　1
　【物件名】　外国語図面　1
　【物件名】　外国語要約書　1
　【物件名】　委任状　1
　　【援用の表示】　平成１５年１１月２０日提出の包括委任状

【書類名】外国語特許請求の範囲

2　WHAT IS CLAIMED IS:

(1) Apparatus of signalling flexible IPMP protection, on server side, comprising the following steps of:

Constructing IPMP Tool List to indicate a list of IPMP tools required for the client to process the media streams within the session; and

Putting the IPMP Tool List into a SDP session level attribute in order to convey the IPMP Tool List to the receiver before media streams start.

(2) Apparatus of signalling flexible IPMP protection, on server side, where IPMP Tool List is constructed and carried as described in claim (1), further comprising the following steps of:

Constructing IPMP Descriptor to indicate which tool is used to protect the media stream, optionally carrying Tool configuration or other types of IPMP data into the IPMP Descriptor; and

Putting the IPMP Descriptor into a SDP session level attribute in order to signal to the receiver that all media streams within the current session is governed by the IPMP Tool described in the IPMP Descriptor.

(3) Apparatus of signalling flexible IPMP protection, on server side, where IPMP Tool List is constructed and carried as described in claim (1), further comprising the following steps of:

Constructing IPMP Descriptor to indicate which tool is used to protect the media stream, optionally carrying Tool configuration or other types of IPMP data into the IPMP Descriptor; and

Putting the IPMP Descriptor into a SDP media level attribute in order to signal to the receiver that the associated media stream is governed by the IPMP Tool described in the IPMP Descriptor.

(4) Apparatus of signalling flexible IPMP protection, on server side, comprising the following steps of:

Carrying usage rights information in IPMP Rights Container; and

Carrying IPMP Rights Container in a session level attribute to indicate that all media streams within the current session are governed by the described usage rules.

(5) Apparatus of signalling flexible IPMP protection, on server side, comprising the following steps of:

Carrying usage rights information in IPMP Rights Data;

Carrying IPMP Rights Data in IPMP Descriptor as a type of IPMP Data; and

Further carrying the IPMP Descriptor in SDP session level attribute to indicate that all media streams within the current session are governed by the described usage rules.

(6) Apparatus of signalling flexible IPMP protection, on server side, comprising the following steps of:

Carrying usage rights information in IPMP Rights Data;

Carrying IPMP Rights Data in IPMP Descriptor as a type of IPMP Data; and

Further carrying the IPMP Descriptor in SDP media level attribute to indicate that the associated media stream is governed by the described usage rules.

(7) Apparatus of signalling flexible IPMP protection, on client side, comprising the following steps of:

Receiving the IPMP Tool List from a SDP session level attribute before media streams start; and

Check the tools indicated in the Tool List, make sure all tools are present in the receiver. If not present, the tools are retrieved, or the playback of media streams is abandoned.

(8) Apparatus of signalling flexible IPMP protection, on client side, where IPMP Tool List is retrieved as described in claim (7), further comprising the following steps of:

Retrieving the IPMP Descriptor from a SDP session level attribute and the client is made known that all media streams within the current session is governed by the IPMP Tool described in the IPMP Descriptor; and

Optionally using the tool configuration data carried in the IPMP Descriptor to configure or initialize the tool, or using other types of data carried in the IPMP Descriptor to assist the IPMP process.

(9) Apparatus of signalling flexible IPMP protection, on client side, where IPMP Tool List is retrieved as described in claim (7), further comprising the following steps of:

Retrieving the IPMP Descriptor from a SDP media level attribute and the client is made known that the associated media stream is governed by the IPMP Tool described in the IPMP Descriptor; and

Optionally using the tool configuration data carried in the IPMP Descriptor to configure or initialize the tool, or using other types of data carried in the IPMP Descriptor to assist the IPMP process.

(10) Apparatus of signalling flexible IPMP protection, on client side, comprising the following steps of:

Retrieving IPMP Rights Container from a SDP session level attribute;

Retrieving usage rights information in IPMP Rights Container; and

Using that to govern all media streams in the current session.

(11) Apparatus of signalling flexible IPMP protection, on client side, comprising the following steps of:

Retrieving IPMP Descriptor from a SDP session level attribute;

Retrieving IPMP Rights Data from the IPMP Descriptor;

Retrieving usage rights information in IPMP Rights Data; and

Using that to govern all media streams in the current session.

(12) Apparatus of signalling flexible IPMP protection, on client side, comprising the following steps of:

Retrieving IPMP Descriptor from a SDP media level attribute;

Retrieving IPMP Rights Data from the IPMP Descriptor;

Retrieving usage rights information in IPMP Rights Data; and

Using that to govern the associated media stream in the current session.

【書類名】外国語明細書

1 TITLE OF THE INVENTION

Apparatus of Signalling Flexible IPMP Protection with Digital Rights Expression in Session Description Protocol

3 DETAILED DESCRIPTION OF THE INVENTION

3.1 Industrial Field of Utilization

The present invention relates to Digital Rights Management (DRM) or Intellectual Property Management and Protection (IPMP) for the generic streaming content protection, especially aims to provide the protection and management of the streaming content where Session Description Protocol (SDP) is used to describe multimedia sessions for the purpose of session announcement, session invitation, and other forms of multimedia session initiation.

3.2 Background and Prior Art

For several years, the promise of delivering video and audio over the Internet interoperably has been widely promoted in the media content distribution industry. Recently, from the standardization point of view, how to protect the media content transmitted from media server to a media client through the IP network and how client's receiver can play the protected media interoperably has also raised much attention. Many standard groups have put tremendous efforts to provide solutions towards this issue.

Internet Streaming Media Alliance (ISMA) is one of such groups. It addresses the need by setting forth a framework for the use of existing open standards that vendors can use to build interoperable video and audio systems for use in IP framework and Internet. ISMA also defines a cryptographic framework, namely ISMACryp, for ISMA media streams. It currently defines a default encryption of media streams and authentication of media messages for ISMA specification and the fmtp signalling of ISMACryp parameters. Figure 1 gives the architecture diagram of ISMACrpt protection over the ISMA framework.

However, such protection specification is quite limited without providing more flexible mechanism to allow different encryption schemes for different content streams or even different protection (e.g. encrypted, watermarked) for the same content stream. It has not provided any mechanism to carry rights information as well.

At the same time, MPEG standardization group has also made much effort on providing a flexible and interoperable IPMP framework for media resource protection. MPEG is working towards to standardize an IPMP framework that involves compliant terminal. All the terminals can represent a protected content that is encrypted and protected by following the same IPMP standard, no matter what kinds of IPMP tools they use. IPMP tools are modules that perform one or more IPMP functions such as authentication, decryption, watermarking, etc. To achieve such a wide interoperability, IPMP provides downloading ability of tools, where tools can be retrieved remotely and renewed with more flexibility. IPMP also allows the terminal to choose its own favourite tool according to parametric description. An IPMP terminal can also aggregate several tools together to form a tool set (act as just one tool) according to some parametric aggregation. Figure 2 shows the general architecture diagram of MPEG IPMP protection.

However, MPEG IPMP framework is defined within MPEG-2/4 system that is not always used for multimedia streaming transmission, although such system can provide more flexible protection scheme.

3.3 Problem to be solved

This invention tries to solve the following problems:

MPEG IPMP provides flexible protection signalling within MPEG-2/4 system. Figure 2 denotes the MPEG-2 IPMP Content Structure and Figure 3 shows the MPEG-4 IPMP Extension Content structure. However, such a flexible protection signalling is not present in media streaming that doesn't used MPEG-2/4 system.

Multimedia streaming over IP using RTP/UDP with RTSP/SDP is more and more popular in current Internet area and end-user can consume such valuable contents more and more easily. SDP can be used to carry plentiful attributes for session level description and media level description to aid such consumption no matter what transport protocol is used to transmit it.

We aim to solve the problem of signalling flexible IPMP protection with rights expression within such popular multimedia streaming environment.

3.4 Means of Solving the Problems

The invention provides the means to use SDP to provide the signalling of flexible IPMP (DRM) protection with rights expression information enforced on actual media stream.

Two additional SDP attributes are defined in this invention to carry flexible IPMP signalling. The defined IPMP related attributes should become mandatory in order to make sure no compliant terminal can skip the copyright protection and management process.

Digital rights information can also be carried in the defined SDP attributes in a normative way. Rights information can be in a variety of forms, including MPEG-21 REL (Rights Expression Language), ODRL (Open Digital Rights Language) etc.

Within the above mentioned SDP attributes, the IPMP Tool List and IPMP Descriptors are utilized to signal the protection. This means is compatible with the latest MPEG-2/4 IPMP Extension standard. It also provides a flexible way to identify IPMP protection tools required to play the streaming content.

3.5 Operation of the Invention

Within the streaming server, IPMP Tool List is constructed based on what types of tools were used to protect the streaming media. The Tool List concept comes from MPEG-2/4 IPMP as shown in 2.1 and 3.1. Here without the presence of either MPEG-2/4 system, this Tool List is carried in the defined SDP attribute "ipmp-control" in the overall session level.

If the streams in the session are governed by some digital rights, which is further expressed in a particular rights language, for example, MPEG-21 REL, the server can put the rights information in IPMP Rights Container which is also carried in "ipmp-control" attributes. In MPEG-2 IPMP, the Rights Container is carried in PSI (Program Specific Information) (2.2), here in SDP, "ipmp-control" attributes is used instead of MPEG-2 system's PSI.

IPMP Descriptors are also constructed based on which tool protects which particular stream. In MPEG-2/4 IPMP, IPMP Descriptors can be carried in various places in MPEG-2/4 system as shown in 2.3 and 3.3. Here these IPMP Descriptors are embedded into the defined SDP attribute "ipmp-d" in each specific media level or the session level in order to signal the tool protection.

Besides tool protection signalling, IPMP Descriptor can also carry all sorts of IPMP_Data_BaseClass derived IPMP Data, including but not limiting to tool configuration, usage rights information, etc.

The SDP is conveyed to the receiver using different transportation protocol, for example, RTSP. The receiver analyzes the defined two IPMP related attributes, namely, "ipmp-control" and "ipmp-d".

Upon detection of IPMP Tool List in "ipmp-control" attribute, the receiver is aware that there is IPMP protection present in the overall session. It make sure all tools announced in the Tool List is available in the terminal before proceeding to play the media streams in the session, and if not, the tools are retrieved from the specified URL.

Upon detection of the digital rights information within IPMP Rights Container in "ipmp-control" attribute, or in IPMP Descriptor in "ipmp-d" attribute in session level, the receiver is aware that all media streams within this current session are governed by the specified digital rights. Appropriate rights enforcement should take place.

Upon detection of IPMP Descriptor in SDP "ipmp-control" attribute in session level, the receiver can be aware of all streams are protected by which tool. And during playback of the streams, the receiver can launch the specified IPMP Tool at specified time and place for all session streams.

Upon detection of IPMP Descriptor in SDP "ipmp-d" attribute in media level, the receiver can be aware of which stream is protected by which tool. And during playback of the streams, the receiver can launch the specified IPMP Tool at specified time and place for specified stream.

The Tool initialization parameters can be carried in the IPMP Descriptor, which can be used to configure the tools before they are actually used. Usage rights information can also be carried in IPMP Descriptor, which can describe the specific usage rules associated with a particular media stream.

3.6 Embodiments

SDP is purely a format for session description – it does not incorporate a transport protocol, and is intended to use different transport protocols as appropriate including the Session Announcement Protocol (SAP), Session Initiation Protocol (SIP), Real-Time Streaming Protocol (RTSP), electronic mail using the MIME extensions, and the Hypertext Transport Protocol (HTTP). It is intended to serve the general purpose so that it can be used for a wider range of network environments and applications for multimedia streaming transmitting.

In general, SDP is a means to communicate the existence of a session, and to convey sufficient information to enable joining and participating in the session. The media information, the timing information and some further information can be described in SDP and distributed by other transport protocol.

A session description consists of a session level description (details that apply to the whole session and all media streams) and optionally several media level descriptions (details that apply onto a single media stream). The session-level part starts with a 'v=' line and continues to the first media level section. The media description starts with a 'm=' line and continues to the next media description or end of the whole session description. In general, session level values are the default for all media unless overridden by an equivalent media-level value.

Attributes (with an 'a=' line) defined in SDP are the primary means for extending SDP. It can be used as "session level" attributes, "media level" attributes, or both. A media description may have any number of attributes ("a=" fields) which are media specific.

These are referred to as "media-level" attributes and can be used to add information about the media stream. Attribute fields can also be added before the first media field; these "session level" attributes convey additional information that applies to the streaming session as a whole rather than to individual media.

In this invention, the characteristics of SDP "attributes" in two different levels will be utilized to signal the flexible IPMP protection. Figure 4 shows the general architecture diagram of flexible IPMP Signalling in SDP. Module 4.1 shows the session level section and 4.2 shows the media level section.

Note: the form of "a=<attribute>:<value>" of "Attribute" fields will be exercised for flexible IPMP signalling.

3.6.1 IPMP Control Information Signalling

Senders should alert receivers that the IPMP control Information session is included by means of an SDP attribute that is general (attribute in session level before any "media" lines). This takes the form of the following attribute line (4.3 in Figure 4):

a=ipmp-control:[<control-data>]

control-data: in an RTSP session, this is an optional attribute. If not supplied, the IPMP Control Information is retrieved over the RTSP session by using DESCRIBE with and an accept of type application/ipmp-control. Where the SDP information is supplied by some other means (e.g. as a file, in SAP), the control-data is obligatory. The control-data should be a URL enclosed in double-quotes, which will supply the IPMP Control Information (e.g. small ones may be encoded using "data:", otherwise "http:" or other suitable file-access URL). The actual IPMP-Control Information is defined in following sub-sections, that including IPMP Tool List followed by Rights Container.

3.6.1.1 IPMP Tool List Class

The IPMP Tool List Class includes a list of IPMP tools. It is used to specify all IPMP tools that should be used in order to play back the content.

Syntax	No. of bits	Mnemonic
IPMPToolList () {		
Length	**16**	**uimsbf**
NumTools	**8**	**uimsbf**
for (i=0; i<numTools; i++) {		
IPMPTool_Info ()		
}		
}		

Semantics of fields in IPMP Tool List Class

- Length – number of bytes of this class, starting immediately following this "Length" field.
- NumTools – This 16 bit field specified how many tools are specified in this IPMP Tool List Class.
- IPMPTool_Info – This class carries information about a tool including its tool ID, possible alternate tools, etc. It is defined as following.

IPMP Tool Info Class

IPMPTool_Info_Class contains information for a logical IPMP Tool required by the Device. The logical tool may be one of the following:
1. A vendor-specific IPMP Tool specified by IPMP_ToolID,
2. One of a list of alternate IPMP Tools,
3. An IPMP Tool specified by a parametric description.

Syntax	No. of bits	Mnemonic
IPMPTool_Info () {		
Length	**16**	**uimsbf**
IPMP_ToolID	**128**	**uimsbf**
isAltGroup	**1**	**uimsbf**
isParametric	**1**	**uimsbf**
Reserved (0b111111)	**6**	**uimsbf**
if (isAltGroup) {		
NumAlternatives	**8**	**uimsbf**
for (i=0; i< numAlternatives; i++) {		
Specific_Tool_ID	**128**	**uimsbf**
}		
}		
if (isParametric) {		
IPMP_ParametricDescription		
}		
numURLs	**8**	**uimsbf**
ToolURL[numURLs]		**ByteArray**
}		

Semantic definitions of fields in IPMP Tool Info Class

Each IPMPTool_Info_Class identifies one IPMP Tool that is required by the terminal to consume the content. This Tool shall be specified either as a unique implementation, as one of a list of alternatives, or through a parametric description.

A unique implementation is indicated by the isAltGroup and isParametric fields both set to zero. In this case, the IPMP_ToolID shall be from the range reserved for specific implementations of an IPMP Tool and shall directly indicate the required Tool.

In all other cases, the IPMP_ToolID serves as a Content-specific abstraction for an IPMP Tool ID since the actual IPMP Tool ID of the Tool is not known at the time of authoring

the Content, and will depend on the Terminal implementation at a given time for a given piece of Content.

A parametric description is indicated by setting the isParametric field to one. In this case, the Terminal shall select an IPMP Tool that meets the criteria specified in the following parametric description. In this case, the IPMP_ToolID shall be from the range reserved for Parametric Tools or Alternative Tools. The actual IPMP Tool ID of the Tool that the terminal implementation selects to fulfill this parametric description is known only to the Terminal. All the Content, and other tools, will refer to this Tool, for this Content, via the IPMP_ToolID specified.

A list of alternative Tools is indicated by setting the isAltGroup flag to "1". The subsequent specific ToolIDs indicate the Tools that are equivalent alternatives to each other. If the isParametric field is also set to one, any Tool that is selected under the conditions for parametric tools (as discussed in the paragraph above) shall be considered by the Terminal to be another equivalent alternative to those specified via specific ToolIDs. The Terminal shall choose one from these equivalent alternatives at its discretion. The actual IPMP Tool ID of this Tool is known only to the Terminal.

- Length – number of bytes of this class, starting immediately following this "Length" field.
- IPMP_ToolID – the identifier of the IPMP Tool.
- isAltGroup – if set to one, this IPMP_Tool contains a list of alternate IPMP Tools.
- numAlternates – the number of alternative IPMP Tools specified in IPMP_Tool.
- Specific_Tool_ID – an array of the IDs of specific alternative IPMP Tools that can allow consumption of the content.
- isParametric – IPMP_Tool contains a parametric description of an IPMP Tool. In this case, IPMP_ToolID is an identifier for the parametrically described IPMP Tool, and the Terminal shall route information specified in the bitstream for IPMP_ToolID to the specific IPMP Tool instantiated by the terminal.
- IPMP_ParametricDescription -- IPMP Parametric Description as defined in the following subclause.
- ToolURL – An array of numURL informative URLs from which one or more tools specified in this class may be obtained.

IPMP Parametric Description Class

Using a parametric description, the content provider can now describe what type of IPMP tool is required to playback the content, instead of using fixed tool IDs. For example, the content provider can specify that an AES tool, with block size of 128 bits is required to decrypt video stream. The IPMP terminal, upon receiving such description specifying this tool, can then choose an optimized AES tool from the embedded tools.

This clause contains an illustration of the hierarchy that a parametric description would follow. It does not attempt to define any specific scheme for any specific Tool type. It is anticipated that such definitions will be added over time to the overall scheme as a need

is identified and an optimal schema developed. We anticipate that only a basic framework will appear in the current version of the specification, and enhancements to the same will be left for future addendums and/or versions.

- Optional comment
- Version of parametric description syntax
- Class of Tool
- e.g. Decryption, Rights Language Parser
- Sub-class of Tool
    - e.g. for Decryption: AES, DES, NESSIE etc
    - e.g. for Watermarking: "Panos's watermarking tool" etc
    - e.g. for Rights Language Parser: "Fred's Rights Parser"
    - e.g. for Protocol Parser: "Mary's Protocol Parser"
- Sub-class-specific information
    - e.g. for DES: number of bits, stream and/or block decipher capability
    - e.g. for Rights Language Parser : version

The parametric description is defined to allow a generic description of any type of IPMP tool, no matter the type of tool.

Syntax	No. of bits	Mnemonic
IPMP_ParametricDescription () {		
Length	16	uimsbf
descriptionComment		ByteArray
majorVersion	8	uimsbf
minorVersion	8	uimsbf
numOfDescriptions	8	uimsbf
for (i=0; i< numOfDescriptions; i++) {		
class		ByteArray
subClass		ByteArray
typeData		ByteArray
type		ByteArray
addedData		ByteArray
}		
}		

Semantic definitions of fields in IPMP Tool Info Class

- class - class of the parametrically described tool, for example, decryption.
- subClass - sub-class of the parametrically described tool, for example, AES under decryption class.
- typeData - specific type data to describe a particular type of tool, for example, Block_length, to further specify a AES decryption tool.
- type - value of the type data above, for example, 128 for the Block_length.
- addedData - Any additional data which may help to further describe the parametrically defined tool.

IPMP Tool ID

The IPMP Tool Identifier is 128-bits long, platform independent, and shall contain a unique identification number for the IPMP Tool. A registration authority for IPMP Tools that use a unique ID is required. (Such registration authority has been defined in MPEG) The registration authority may further maintain an association of the download URLs for various implementations of the given tool for various platforms. These platforms will be described to adequate detail using a structured representation. The IPMP ToolID identifies a specific IPMP Tool, unless in the reserved range for parametrically defined tools or alternative tools. Specific values within this 128-bit space are reserved for indicating parametric tools, the bitstream, the terminal, and other special addresses. These values may not be assigned to registered Tools.

IPMP_ToolID	Semantics
0x0000	Forbidden
0x0001	Content
0x0002	Terminal
0x0003 - 0x2000	Reserved for ISO use
0x2001 - 0xFFFF	Carry over from 14496-1 RA
0x10000 - 0x100FF	Parametric Tools or Alternative Tools
0x100FF – 2^128-2	Open for registration
2^128-1	Forbidden

3.6.1.2 IPMP Rights Container Class

IPMP Rights Container Class conveys the usage rules & states associated with the IPMP protected content.

Syntax	No. of bits	Mnemonic
IPMP_Rights_Container () {		
Length	**16**	**uimsbf**
rights_data		**ByteArray**
}		

Semantic Definitions of Fields in IPMP Rights Container Class

- Length – number of bytes of this class, starting immediately following this "Length" field.
- rights_data – This contains the details of usage rights information. It can carry the actual MPEG-21 REL or OMA ODRL data.

3.6.2 Signalling of IPMP Descriptor

Senders should also alert receivers that the IPMP specific descriptor is included by means of an SDP attribute that can be associated with each specific media stream (attribute in media level) or the entire session. This takes the form of the following attribute line (4.4 in Figure 4):

a=ipmp-d:[<descriptor-data>]

descriptor-data: in an RTSP session, this is an optional attribute. If not supplied, the IPMP Descriptor is retrieved over the RTSP session by using DESCRIBE with and an accept of type application/ipmp-d. Where the SDP information is supplied by some other means (e.g. as a file, in SAP), the description-data is obligatory. The description-data should be a URL enclosed in double-quotes, which will supply the IPMP Control Information (e.g. small ones may be encoded using "data:", otherwise "http:" or other suitable file-access URL). The actual IPMP Descriptor is defined in following sub-sections.

The presence of IPMP Descriptor indicates the associated media stream is protected by the IPMP Tool described in the IPMP Descriptor.

The presence of IPMP Descriptor at session level indicates that all media streams in the current session is protected by the IPMP Tool described in the IPMP Descriptor.

3.6.2.1 IPMP Descriptor

Syntax	No. of bits	Mnemonic
IPMP_descriptor() {		
descriptor_tag	8	Uimsbf
descriptor_length	8	Uimsbf
IPMP_Descriptor_ID	32	Uimsbf
IPMP_ToolID	128	Uimsbf
ControlPoint	8	uimsbf
SequenceCode	8	uimsbf
IPMP_Data_length	16	uimsbf
for (i=0; I< N; i++) {		
IPMP_Data		
}		
IsSigned	8	Uimsbf
if (isSigned)		
Signature		ByteArray
NumCerts	8	uimsbf
for (i=0; i<numCerts;i++) {		
CertType	8	uimsbf
Certificate		ByteArray
}		
Verifying_Tool_ID	128	uimsbf
}		
}		

Semantic Definitions of Fields in IPMP Descriptor

- IPMP_Descriptor_ID – a unique ID of this IPMP descriptor. This could be used to refer to this particular descriptor. 0x00000000 and 0xFFFFFFFF are prohibited.

Since an IPMP Tool's instantiation is signalled by a unique IPMP Descriptor, this IPMP_Descriptor_ID can also used as a unique identification of an IPMP Tool instance for messaging.

- IPMP_ToolID – Unique ID of the IPMP Tool that is protecting in this scope.
- controlPoint – value specifying the IPMP control point at which the IPMP Tool resides, and is one of the following values:

Terms of TB_n, B_n, EB_n, D_n are defined in STD model of MPEG-2 Systems ISO/IEC 13818-1.

Control Point	Description
0x00	No control point.
0x01	Control Point after Transport Buffer
0x02	Control Point between the decode buffer and the decoder
0x03	Control Point between the decoder and the rendering.
0x04 - 0xDD	reserved
0xDE - 0xFE	User private
0xFF	Forbidden.

- sequenceCode - value specifying the relation of the IPMP Tool to IPMP Tool(s) residing at the same control point. The value of this field specifies the priority of this IPMP Tool at this specific control point. For example, a value of "20" means this tool has a higher priority than an IPMP tool with sequenceCode "12". Data will be routed to the IPMP tool with a higher priority first, before the data goes to the next lower priority IPMP tool. Two tools shall not have the same sequence number at the same control point for the same stream.
- IPMP_Data -- The IPMP Data that is extended from IPMP_Data_BaseClass as defined in ISO 13818-11. The IPMP Data includes but not limited to IPMP Rights Data, IPMP Key Data, Tool Configuration Data, etc.
- isSigned – This 1 bit field indicates the presence of a signature in the IPMP Descriptor.
- Signature – The signature of the entire IPMP Descriptor.
- CertType – The type of certification mechanism being used, value assigned by a Registration Authority.
- NumCerts – The number of certificates included.
- Certificate -- The array of certificates.
- Verifying_Tool_Id – The ID of the Tool that is required to verify the certificate(s). A value of 0 indicates the device.

3.6.3 Example

The following is an example of flexible IPMP protection signaling in SDP, which is carried in an RTSP session.

Client Request for an FGS bitstream

C->S

DESCRIBE rtsp://140.113.211.184/foreman.m4v RTSP/1.0

CSeq: 0
User-Agent: PSL FGS Player: 176x144, 16-bit color, FGS, 10
Accept: application/sdp

S->C

RTSP/1.0 200 OK
CSeq: 0
Content-Type: application/sdp
Content-Length: 529

v=0
o=StreamServer 10608739570467017277 1016147297000 IN IP4 140.113.211.184
s=PSL mpeg4 stream
e=server@psl.com.sg
c=IN IP4 140.113.211.184
t=0 0
a=control:*
a=range:ntp=0- 7.40000
a=ipmp-control: "http://aaa.com/ipmp"

m=video 0 RTP/AVP 96
a=rtpmap:96 MP4V-ES/90000
a=control:trackID=0
a=fmtp:96 profile-level-id=17; config=000001010000012002044007a82c2090a21f

m=video 0 RTP/AVP 97
a=rtpmap:97 MP4V-ES/90000
a=control:trackID=1
a=fmtp:97 profile-level-id=18;
config=000001010000012189285001ec705841217ffb6db6b6db6db6c924920f
a=depends_on:trackID=0
a=ipmp-d: "data:application/ipmp-d;base64,
VndCTFFVZkF5a0F5U1FBWlFRTklCRUFIMEFBQVBvQUFBRDZBQVlRQUVR
QUFBUG9BAAAA"

(C->S denote RTSP message sending from client to server; S->C denote RTSP message sending from server to client.)

The above example shows that the receiver should retrieve IPMP Control Information (IPMP Tool List and Rights information) from a HTTP site (http://aaa.com/ipmp), which is represented in session level attribute of SDP declaration. In the media session level, the FGS base layer video stream is not protected but the enhancement layer video is protected by one IPMP tool whose description is carried in IPMP Descriptor and encoded in Base64 which is further declared in SDP second media attribute.

3.7 Effects of Invention

The invention uses the IPMP Tool List and Rights Container in session level attribute of SDP and IPMP Descriptors in either media level or session level attribute of SDP to signal flexible IPMP protection with rights information for the streaming content.

By doing so, the followings have been achieved:

- Indicate what IPMP Tools are need in order to join the overall session and playback all media streams by the use of IPMP Tool List in session level attribute "IPMP-Control".
- Indicate what is the usage rights associated with the entire session by using IPMP Rights Container in session level attribute "IPMP-Control"
- Indicate which IPMP Tool protects which media stream by using IPMP Descriptor in media level or session level attribute "IPMP-D".
- Send tool configuration data, specific media level usage rights information, key data in the IPMP_Data field of IPMP Descriptor.

"ipmp-control" and "ipmp-d" SDP attributes defined in this invention can achieve a full flexible IPMP signaling. Hence terminal side is able to implement flexible and secure IPMP framework by following what is described in 13818-11 or 14496-13 (MPEG-2/4 IPMP Extension).

4 BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 shows ISMACryp Architecture

Figure 2 shows the MPEG-2 IPMP Extension content structure

Figure 3 shows the MPEG-4 IPMP Extension content structure.

Figure 4 shows the IPMP protection signalling using SDP attributes

【書類名】外国語図面

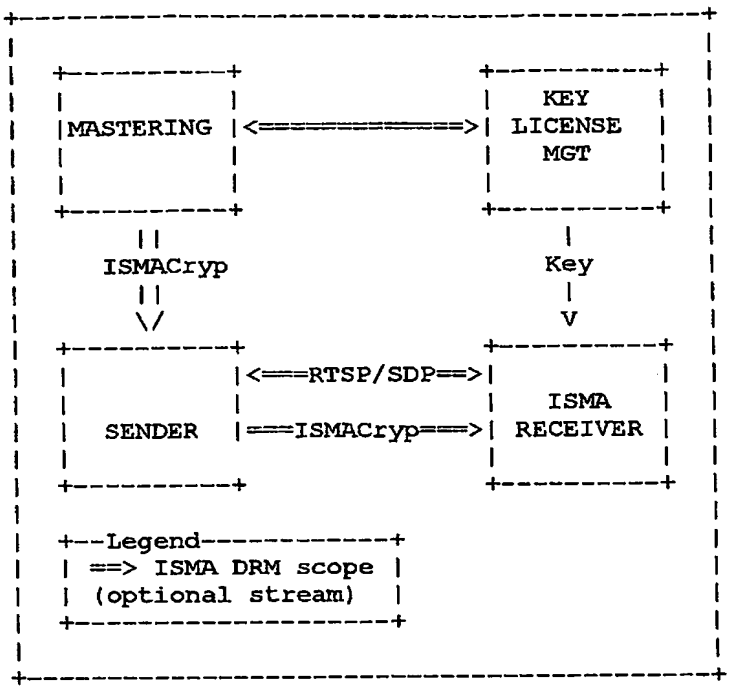


Figure 1

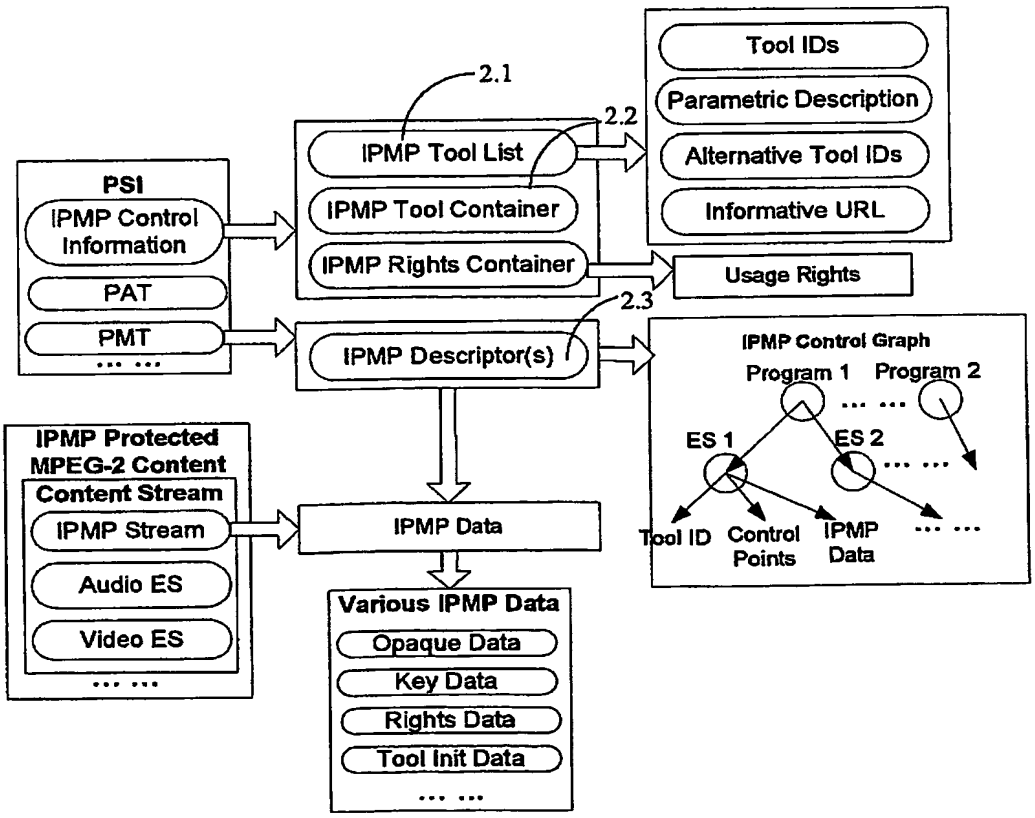


Figure 2

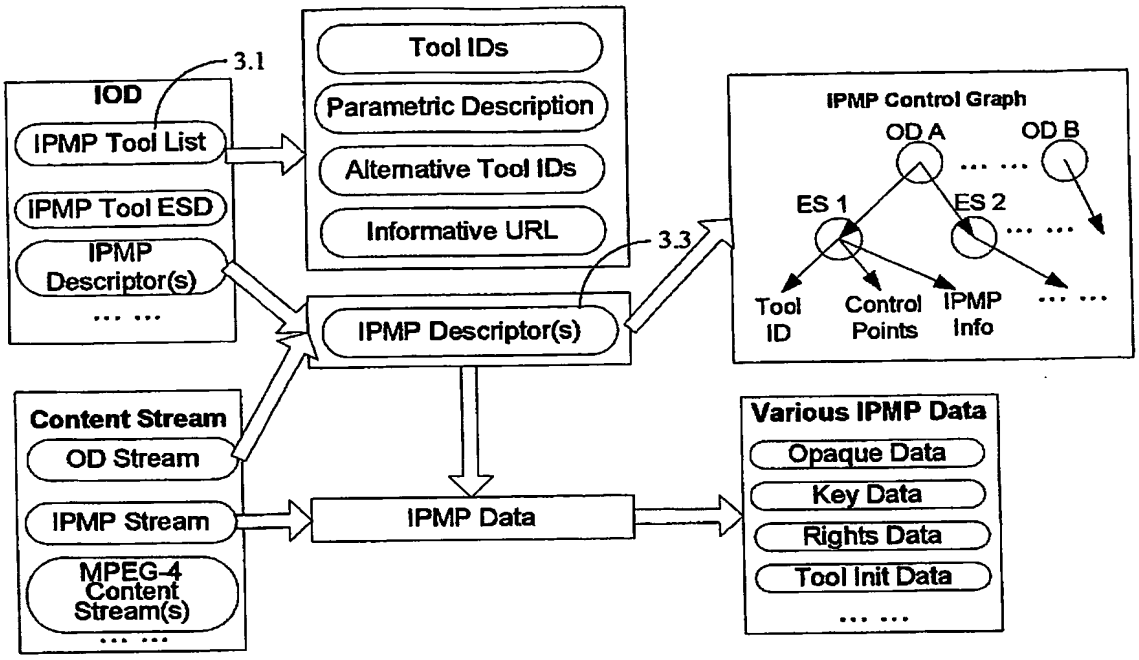

IOD
3.1
IPMP Tool List
IPMP Tool ESD
IPMP Descriptor(s)
... ...
Tool IDs
Parametric Description
Alternative Tool IDs
Informative URL
3.3
IPMP Descriptor(s)
IPMP Control Graph
OD A
OD B
ES 1
ES 2
Tool ID
Control Points
IPMP Info
Content Stream
OD Stream
IPMP Stream
MPEG-4 Content Stream(s)
IPMP Data
Various IPMP Data
Opaque Data
Key Data
Rights Data
Tool Init Data

Figure 3

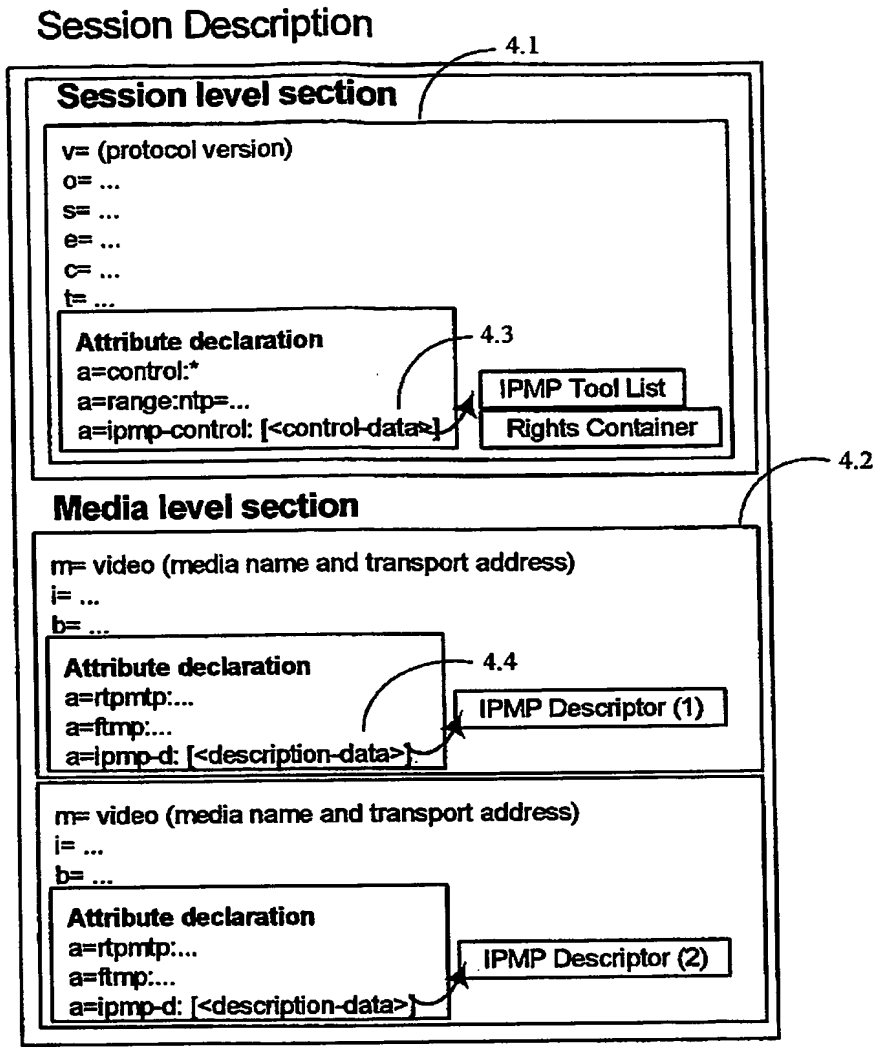

Session Description
4.1
Session level section
v= (protocol version)
o= ...
s= ...
e= ...
c= ...
t= ...
Attribute declaration
a=control:*
a=range:ntp=...
a=ipmp-control: [<control-data>]
4.3
IPMP Tool List
Rights Container
4.2
Media level section
m= video (media name and transport address)
i= ...
b= ...
Attribute declaration
a=rtpmtp:...
a=ftmp:...
a=ipmp-d: [<description-data>]
4.4
IPMP Descriptor (1)
m= video (media name and transport address)
i= ...
b= ...
Attribute declaration
a=rtpmtp:...
a=ftmp:...
a=ipmp-d: [<description-data>]
IPMP Descriptor (2)

Figure 4

【書類名】外国語要約書

6 ABSTRACT

This invention defines how the flexible IPMP protection signalling and rights information should be carried and conveyed to the receiver using SDP attributes. A SDP specific attribute IPMP-Control on session level can be used to carry the overall IPMP Control Information for the whole session including IPMP Tool List and Rights Container. The other SDP specific attribute IPMP-D on either media level or session level can be used to carry the individual IPMP descriptor associated with some individual media stream to indicate the IPMP protection on media level.

特願２００３－４０１３８３

出　願　人　履　歴　情　報

識別番号　［０００００５８２１］

１．変更年月日　１９９０年　８月２８日
［変更理由］　新規登録
住　所　大阪府門真市大字門真１００６番地
氏　名　松下電器産業株式会社

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP04/017602

International filing date: 26 November 2004 (26.11.2004)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2003-401383
Filing date: 01 December 2003 (01.12.2003)

Date of receipt at the International Bureau: 27 January 2005 (27.01.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse